



# IRISH RAILWAY RECORD SOCIETY

## Data Protection Policy of the Irish Railway Record Society

### Purpose of our Policy

The Irish Railway Record Society Company Limited by Guarantee ("the Society"), in its capacity as a data controller and data processor, has a legal obligation to comply with the Data Protection Acts and the EU General Data Protection Regulation.

### Scope of our Policy

This policy applies only to the Society's activities in Ireland. The Society's activities in the United Kingdom will be governed by a separate policy compliant with the applicable law in that jurisdiction and in keeping with the general approach set out in this document.

The Society has a legitimate need to collect and retain personal data in relation to its members and other persons. This "legitimate need" includes the provision of services to members, the operation of events and trips for members and guests and compliance with law. The Society also holds personal data in its archives, principally the employment records of former railway employees which are retained for archival and historical research purposes. It has therefore adopted the following policy governing the collection, retention, processing and use of that personal data.

This policy applies to all personal data held by the Society, whether held in electronic or paper format. "Personal data" means data relating to a living person who is or can be identified either (a) from the data or (b) from the data in conjunction with other information in the possession of the Society or likely to come into its possession.

This policy applies to, and is to be fully implemented by, the members of the Board and by persons carrying out functions on behalf of the Society.

### Description of Personal Data Held and the Purposes for which it is Processed by the Society

**Members:** The Society holds and processes the following personal data in relation to its members: name, membership number, postal address, email address, date of birth (if under 21), category of membership and method of payment (cash, cheque, Paypal etc.). The Society does not retain any personal financial information (such as account or card numbers) relating to its members. The personal data is used to give notice and provide information to members required by law and/or the Society's constitution, to send the Society's Journal and other publications to members and to inform members about Society events and activities. The personal data of members is **not** shared with or given to any third

party, but the Society may itself communicate with members about third party events, activities or publications relevant to the objects of the Society. Personal data is retained as long as a person remains a member of the Society and for a period of two years after they cease to be members, to enable them to retain the option of re-applying for membership under Article 9(c) of the Society's constitution. The persons primarily responsible for processing this personal data are the Hon. Membership Secretary and the Hon. Treasurer.

**Event Participants:** Members of the Society and non-members may participate in Society events and activities (such as rail trips). The Society holds and processes the following personal data in relation to participants: name, membership number (if applicable), postal address, email address, telephone number and method of payment (cash, cheque, Paypal etc.). The Society does not retain any financial information (such as account or card numbers) relating to participants. The personal data is used to record payment and to communicate with participants about the event or activity and is deleted/disposed of in a secure manner following the event. However, in the case of non-members, their personal data may be retained **with their explicit consent** solely for the purpose of communicating with them about future events, activities or publications relevant to the Society's objects. The persons primarily responsible for processing this personal data are the Hon. Programme Officer and the Hon. Treasurer.

**Archives:** The Society holds the employment records of some former railway employees for archival and historical research purposes. The Society holds and processes the following personal data in relation to those former employees: name, address, date of birth, date entered railway service, wages paid, date of retirement, resignation and/or death and disciplinary records for certain categories of employees. The Society will apply the following criteria to the processing of this personal data in accordance with the Principles of Access to Archives of the International Council on Archives and good archival practice:

- Subject to the limited exceptions outlined below, access to this personal data will be closed for a period of seventy years from the date the records were accepted into the Society's archives.
- The Society may process this personal data to the extent necessary for good archival practice, including but not limited to safe and secure storage, digitisation of the records and deletion of special categories of data (such as information concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, health, sexual orientation or trade union membership).
- The Society may permit processing for bona fide research purposes where this personal data is pseudonymised, that is processed in such a way that the data can no longer be attributed to a specific person.
- Any person whose personal employment records are held by the Society may access those records once they have provided satisfactory proof of identity. They may also authorise in writing other persons to access their records.
- A direct relative (such as a spouse or civil partner, brother or sister, child or grandchild) of a deceased person whose personal employment records are held by the Society may access those records on production of (a) a death certificate, (b) satisfactory evidence of their direct relationship with the deceased person and (c) satisfactory proof of their own identity.

Processing of archival data will respect the principle of data minimisation, which means it will only be processed where it is essential to do so and then only to the minimum extent necessary and pseudonymised where possible. Except where the data are processed at the request of the person themselves or a direct relative, processing will avoid the identification of data subjects.

The persons primarily responsible for processing this personal data are the Hon. Archivist and the archives team.

**Journal Recipients and Event Invitees:** A limited number of non-members receive copies of the Society's Journal on an ex-gratia basis. A limited number of persons are invited to attend Society events, particularly the annual dinner. The Society holds and processes the following personal data solely for these purposes: name, address and email address. The personal data is deleted/disposed of in a secure manner when they are no longer sent copies of the Journal or no longer invited to Society events. The persons primarily responsible for processing this personal data are the Hon. Membership Secretary and the Secretary.

### **Principles of our Data Protection Policy**

The Society will observe the following principles in relation to personal data. It will:

- Obtain and process the personal data lawfully, fairly and in a transparent manner. That includes ensuring that members, participants in Society events/activities, Journal recipients and event invitees from whom data is being collected and processed are aware of the reasons for collecting/processing it, of the persons to whom it may be disclosed and of the right to access their own data.
- Process the personal data only for specific, legitimate and explicit purposes and in a way which is compatible with those purposes.
- Ensure that the data is adequate, relevant and not excessive in relation to the purposes for which it is processed.
- Only process the personal data of members, participants in Society events/activities and Journal recipients and event invitees with their explicit, freely given, specific, informed and unambiguous consent. Model forms of consent are to be found in the Annex. The employment records of former railway employees are held for archival and historical research purposes and are considered to be exempt from the consent requirements.
- Only obtain and process the personal data of persons under eighteen years of age with the explicit consent of their parent or guardian.
- Use or disclose the data only in ways which are compatible with the purposes for which it was collected. This means that personal data will not be used for a purpose other than that for which it was originally collected.

- Keep the personal data safe and secure, whether held in electronic or paper format.
- Keep the personal data accurate, complete and up-to-date.
- Ensure that the personal data is adequate, relevant and not excessive. Only the minimum amount of data which is needed for a particular purpose will be sought and retained.
- Retain the personal data for no longer than is necessary for the purposes for which it was collected. If the purpose for which the data was originally obtained has ceased and the personal data is no longer required, it will be deleted or disposed of in a secure manner.
- Ensure that personal data will not be shared with or given to any third party, subject to the exception that the Society may itself communicate with members about third party events, activities or publications relevant to the objects of the Society.
- Give a copy of his or her personal data to a person on request and rectify, supplement, restrict processing or delete/dispose of it in a secure manner upon request.

The Society will not transfer any personal data outside the European Economic Area (EU, Norway, Iceland and Liechtenstein) without familiarising itself and complying with any special conditions governing such transfer.

Detailed guidance in relation to the application of these principles is available on the website of the Data Protection Commission <http://www.dataprotection.ie>.

### **Data Protection Officer**

To ensure compliance with the Data Protection Acts, the EU General Data Protection Regulation and the implementation of this policy, the Board has designated Denis Moran as Data Protection Officer. The functions of the Data Protection Officer include:

- monitoring compliance with the Data Protection Acts, the EU General Data Protection Regulation, this policy and the CCTV Data Protection Policy;
- providing advice and assistance on the implementation of the law and this policy;
- acting as a point of contact with the Data Protection Commission and cooperating with it.
- acting as a point of contact for access and rights requests under the law.

### **Our Undertakings on Data Protection**

The Society in Ireland will ensure that:

- Members of the Board and other persons carrying out functions on behalf of the Society are made aware of the requirements of the Data Protection

Acts and the EU General Data Protection Regulation, of this policy, of the CCTV Data Protection Policy and of any other more detailed guidance on data protection which may be prepared by the Society.

- Persons who have particular responsibility for the processing and use of personal data are fully aware of their obligations under the Data Protection Acts, the EU General Data Protection Regulation and this policy.
- This policy and any associated guidance is reviewed and updated at least every two years, so that data protection is a “living” process aligned to the way the Society conducts its business.
- There is a regular review of the accuracy, security and continuing need for, and relevance of, the personal data held by the Society.
- There is a clear allocation of responsibility for compliance with the Data Protection Acts, the EU General Data Protection Regulation and this policy.
- It adheres to the “need to know principle” – only personal data necessary for the particular purpose should be collected and persons should only be able to access the personal data that they need to carry out their functions.
- It has adequate access controls, firewalls and virus protection for electronic data. Paper records are securely stored.
- There are periodic audit checks to ensure that the Society is complying with the Data Protection Acts and this policy.
- There is a Data Protection Statement on the Society’s website and on forms used by the Society.

### **Our Commitments on Data Security**

Members of the Board and persons carrying out functions on behalf of the Society are responsible for ensuring, in their respective spheres of activity, that:

- Any personal data that they hold, whether in electronic or paper format, is kept securely.
- Personal data is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.
- Items that are marked “personal” or “private and confidential”, or appear to be of a personal nature, are only opened by the addressee or a person authorised by them to do so.
- Access to information is restricted to members of the Board and other authorised persons on a “need-to-know” basis.
- Paper files with personal information are stored in locked filing cabinets.
- Electronic data that contains personal information is held in password protected files with access permitted to a limited number of users.

- Personal data on computer screens or paper files is not accessible by visitors to the Society's premises or at any other location.
- Waste paper and printouts containing personal data are carefully disposed of.
- Any data which is no longer required is disposed of carefully and thoroughly.
- The Society's premises are secured when unoccupied.

### **Processing of Requests for Access to Personal Data**

The Society will ensure that that it follows the relevant law and the guidelines on access to personal data set down by the Data Protection Commission. Every person about whom the Society keeps personal data has a right to request a copy of the data which is kept about them.

On making an access request, any person about whom the Society holds personal data is entitled to:

- a copy of the data we are keeping about him or her;
- know the categories of their data and our purpose/s and legal basis for processing it;
- know the identity of persons to whom we disclose the data;
- the period for which the data will be retained or the criteria used to determine the period;
- know the origin of the data, unless it is contrary to public interest;
- know the logic involved in automated decisions;
- a copy of data held in the form of opinions, except where such opinions were given in confidence. However, in cases where the person's fundamental rights suggest that they should access the data in question, it should be given.

Every person about whom the Society keeps personal data has a number of other rights under the Data Protection Acts and the EU General Data Protection Regulation (GDPR), in addition to the right of access. These include:

- the right to have inaccuracies corrected (Article 16 of GDPR);
- the right to have their personal data erased (Article 17 Of GDPR);
- the right to object to the use of their personal data for direct marketing (which the Society does not do);
- the right (under Article 18 of GDPR) to restrict the processing of their personal data, including automated decision making (the Society does not use automated decision making);
- the right to withdraw consent to the continued processing of their personal data;
- the right to make a complaint to the Data Protection Commission at <http://www.dataprotection.ie> or (057) 868400 or (0761) 104800.

To make an access request or exercise any other right, a person must:

- Apply in writing (which can include email) to the Society's Data Protection Officer, any member of the Board or send a message to [dataprotection@irrs.ie](mailto:dataprotection@irrs.ie);
- Give any details which might be needed to help the Society identify him/her and locate all the information we may keep about him/her e.g. previous addresses, information on age, etc.;

In response to an access request the Society must:

- Supply the information to the person promptly and within one month of receiving the request but it may before the end of that month extend the period by up to a further two months taking into account the complexity of the request and the number of such requests received;
- Provide the information in a form which will be clear to the ordinary person.

If the Society restricts a person's right of access to their personal data in accordance with the provisions of the Data Protection Acts or the EU General Data Protection Regulation, the Society will notify that person within one month and inform them of the reasons for the decision and of their right to complain to the Data Protection Commission at <http://www.dataprotection.ie> or (057) 868400 or (0761) 104800. Information on the restrictions on the right of access is available on <http://www.dataprotection.ie>.

The Society will also respond to other requests within one month confirming the action it has taken to comply with the request.

### **Our Response to Data Breaches**

Any person who becomes aware of an actual or suspected breach of personal data held by the Society should at the first available opportunity notify the Data Protection Officer at or any other member of the Board or send a message to [dataprotection@irrs.ie](mailto:dataprotection@irrs.ie).

Where a data breach is discovered or reported, the Data Protection Officer and any other relevant officer of the Society will immediately carry out an investigation:

- To ascertain the extent of the breach, the approximate number of data subjects and personal records affected and the type of personal data involved;
- To identify the cause of the breach, its likely consequences and measures to mitigate and resolve the breach;
- To identify possible adverse effects on data subjects affected by the breach and particularly whether the breach is likely to result in a risk to the rights and freedoms of data subjects affected and to identify measures to mitigate these adverse effects.

With the assistance of the Data Protection Officer and any other members of the Board, the relevant officer will implement the measures identified to (a) mitigate and resolve the breach and (b) to mitigate any adverse effects on affected data subjects. Where the data breach is considered serious and/or where the cost of

the mitigation measures is likely to be significant, the Data Protection Officer is authorised to call an emergency meeting of the Board or to seek Board decisions by written procedure.

The Data Protection Officer will maintain a written record of the outcome of the investigation and of the measures implemented. He will keep the Board informed of material developments.

Where the data breach is likely to result in a risk to the personal rights and freedoms of data subjects, the Data Protection Officer will notify the Data Protection Commission without undue delay and where feasible within 72 hours of the Society becoming aware of the breach and provide the information required by law.

Where the data breach is likely to result in a **high** risk to the personal rights and freedoms of data subjects, the Data Protection Officer will notify the data subjects to whom the breach relates without undue delay and provide them with the information required by law. However, a notification is not required by law where the Society has taken measures that ensure that the high risk to the rights and freedoms of the affected data subjects is no longer likely to materialise. Where the notification to affected data subjects would involve disproportionate effort, the Data Protection Officer may notify them by way of a public communication or other similar measure that ensures they are informed in an equally effective manner.

### **Updating and Review of our Policy**

This policy will be updated at least every two years and more frequently if required to reflect best practice in data management, security and control and to ensure compliance with any amendments made to the Data Protection Acts and relevant EU legislation.

**Approved by the Board on 17 May 2018**

**Next Review Date: May 2020**